UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/552,586	10/12/2005	Masato Yamamichi	2005_1537A	2279

52349 7590 09/17/2010
WENDEROTH, LIND & PONACK L.L.P.
1030 15th Street, N.W.
Suite 400 East
Washington, DC 20005-1503

EXAMINER	
TRUVAN, LEYNNA THANH	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
09/17/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ddalecki@wenderoth.com
eoa@wenderoth.com

Office Action Summary	**Application No.** 10/552,586	**Applicant(s)** YAMAMICHI ET AL.	
	Examiner Leynna T. Truvan	**Art Unit** 2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 July 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14 and 17-37* is/are pending in the application.

4a) Of the above claim(s) *15 and 16* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14 and 17-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-14, 17-37 are pending.

2. Claims 25, 29, 34, and 37 have overcome the rejection under 35 U.S.C. 101, thus are now withdrawn.

Response to Arguments

3. Applicant's arguments filed 7/2/10 have been fully considered but they are not persuasive.

Regarding the argument on pg. 25, the feature of claim 1 is not disclosed or suggested by the Hoffstein and Irvin combination. Hoffstein discloses encoding and decoding of information, more particularly, a public key cryptosystem for encryption and decryption of digital messages by processor system (col.1, lines 15-19). The invention allows keys to be chosen essentially at random from a large set of vectors, with key lengths comparable to the key lengths in other common public key cryptosystems, and features an appropriate security level, and provides encoding and decoding processes which are between one and two orders of magnitude faster than the most widely used public cryptosystem, namely the exponentiation cryptosystem (col.2, lines 45-53). Additionally, specification (pgs.2-4) discloses the NTRU Cryptosystems, Inc. is a trademark by Hoffstein et al. and teaches Document 2 which admits the NTRU as prior art known to use non-negative integer parameters, polynomial ranges to avoid the occurrence of decryption errors. Thus, the Hoffstein reference suggests (col.6-col.12) the current amendment "wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non-negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem", for the fifth type of trap door function which has been used to create public key cryptosystems is based on error correcting codes (col.2, lines 14-21).

As for Irvine, includes an error check value generation circuit based on the unencrypted message and adds the error check value to the encrypted message (col.6, lines 45-50). Irvine discloses generating an error check value for the decrypted message can determine if there is no error. The error check value for the decrypted message can indicate no error message (col.4, lines 30-46 and col.11, lines 10-12). Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Hoffstein with Irvin to teach generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error because to selectively encrypt and decrypt messages transmitted on the communication network by generating error check value for the decrypted message indicates no error (Irvin - col.4, lines 30-46 and col.11, lines 10-12).

Regarding the argument on pg. 26 for claims 18-37, which is similar to claim 1. The arguments are addressed above.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-14, 17-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hoffstein, et al. (US 6,298,137), in view of Irvin (US 6,832,314).

As per claim 1:

Hoffstein discloses a parameter generation apparatus for generating an output parameter, the output parameter being a set of parameters causing no decryption error for an NTRU cryptosystem, the parameter generation apparatus comprising:

an error-free output parameter generation unit operable to generate the output parameter causing no decryption error based on error condition information that is provided in advance, the error condition information indicating a condition for causing no decryption error:

wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and

wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial f whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem. (col.9, lines 44-67 and col.10, lines 25-52 and col.11, lines 10=-55)

Hoffstein, ET al. is inventors for NTRU Cryptosystems, Inc. Hoffstein discloses encoding and decoding of information, more particularly, a public key cryptosystem for encryption and decryption of digital messages by processor system (col.1, lines 15-19). The invention allows keys to be chosen essentially at random from a large set of vectors, with key lengths comparable to the key lengths in other common public key cryptosystems, and features an appropriate security level, and provides encoding and decoding processes which are between one and two orders of magnitude faster than the most widely used public cryptosystem, namely the exponentiation cryptosystem (col.2, lines 45-53). Hoffstein further discusses. The Hoffstein reference suggests (col.6-col.12) the current amendment “wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem”, for the fifth type of trap door function which has been used to create public key cryptosystems is based on error correcting codes (col.2, lines 14-21).

However, did not further include generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error.

Irvine includes an error check value generation circuit based on the unencrypted message and adds the error check value to the encrypted message (col.6, lines 45-50). Irvine discloses generating an error check value for the decrypted message can determine if there is no error. The error check value for the decrypted message can indicate no error message (col.4, lines 30-46 and col.11, lines 10-12).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Hoffstein with Irvin to teach generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error because to selectively encrypt and decrypt messages transmitted on the communication network by generating error check value for the decrypted message indicates no error (Irvin - col.4, lines 30-46 and col.11, lines 10-12).

As per claim 2: See Hoffstein on col.10, lines 35-40 and Irvin on col.4, lines 30-46 and col.11, lines 10-12; discussing the parameter generation apparatus according to claim 1, wherein the error-free output parameter generation unit includes: a provisional parameter generation unit operable to generate a set of provisional parameters <u>causing no decryption error</u> based on the error condition information; and an output parameter generation unit operable to generate the output parameter, using the set of provisional parameters, based on a lattice constant that is calculated from the set of provisional parameters.

As per claim 3: See Irvin on col.4, lines 30-46 and col.11, lines 10-12; discussing the parameter generation apparatus according to claim 2, wherein the provisional parameter generation unit generates the set of provisional parameters causing no decryption error based on an input parameter and the error condition information, the input parameter being a set of parameters for the NTRU cryptosystem that are inputted from outside.

As per claim 4: See Hoffstein on col.5, lines 10-20; discussing the parameter generation apparatus according to claim 2, wherein the output parameter generation unit generates the output parameter, using the set of provisional parameters, based on security determination information and security level information, the security determination information being associated with the lattice constant, and the security level information indicating a level of security against decryption performed by a third party.

As per claim 5: See Hoffstein on col.5, lines 10-20 and col.10, lines 35-40; discussing the parameter generation apparatus according to claim 4, wherein the output parameter generation unit includes a security determination information holding unit operable to hold the security determination information, and wherein the security determination information is provided from outside.

As per claim 6: See Hoffstein on col.10, lines 35-40; discussing the parameter generation apparatus according to claim 4, wherein the output parameter generation unit includes a lattice constant storage unit operable to store one or more lattice constant and security determination information pairs, and wherein the lattice constant and the security determination information are provided from outside.

As per claim 7: See Hoffstein on col.10, lines 35-40 and Irvin on col.4, lines 30-46 and col.11, lines 10-12; discussing the parameter generation apparatus according to claim 6, wherein the output parameter generation unit further includes a security determination information selection unit operable to select security determination information from the one or more lattice constant and security determination pairs stored in the lattice constant storage unit, based on the lattice constant, and the output parameter generation unit generates the output parameter, using the selected security determination information and the lattice constant that is paired with the selected security determination information.

As per claim 8: See Hoffstein on col.10, lines 35-40 and Irvin on col.4, lines 30-46; discussing the parameter generation apparatus according to claim 6, wherein the output parameter generation unit includes: a modification judgment unit operable to judge whether to modify the set of provisional parameters, based on the lattice constant and the security determination information; a provisional parameter modification unit operable to generate a modified set of provisional parameters using the set of provisional parameters, when the modification unit judges that the set of provisional parameters should be modified; and a generation unit operable to generate the output parameter, using the modified set of provisional parameters, based on the security level information.

As per claim 9: See Hoffstein on col.7, lines 4-50 and col.9, lines 24-40; discussing the parameter generation apparatus according to claim 8, wherein the provisional parameter modification unit generates the modified set of provisional parameters by modifying a non-negative integer dg, included in the set of provisional parameters, for specifying the number of coefficients in a random polynomial g whose coefficient values equal to 1, the random polynomial g being used for generating a public key polynomial.

As per claim 10: See Hoffstein on col.4, lines 14-30 and col.9, lines 48-55; discussing the parameter generation apparatus according to claim 2, wherein the set of provisional parameters and the output parameter are each made up of a set of the following: a degree N in the NTRU cryptosystem; the non-negative integer p; the non-negative integer q; the non-negative integer df for specifying the number of coefficients in a private key polynomial f whose coefficient values equal to 1; the non-negative integer dg for specifying the number of coefficients in a random polynomial g whose coefficient values equal to 1, the random polynomial g being used for generating a public key polynomial; and the non-negative integer d for specifying the number of coefficients in a random number polynomial r whose coefficient values equal to 1, the random number polynomial r being used for encrypting a plain text.

As per claim 11: See Hoffstein on col.5, lines 10-20 and col.10, lines 25-40; discussing the parameter generation apparatus according to claim 10, wherein the provisional parameter generation unit includes an initial security determination information holding unit operable to hold initial security determination information that is associated with time needed to perform decryption, and wherein the provisional parameter generation unit generates the degree N included in the set of provisional parameters, based on the security level information and the initial security determination information.

As per claim 12: See Hoffstein on col.4, lines 14-30 and col.9, lines 48-55; discussing the parameter generation apparatus according to claim 10, wherein the provisional parameter generation unit generates the non-negative integer df, the non-negative integer dg, and the non-negative integer d that are included in the set of provisional parameters, based on the security level information and the degree N.

As per claim 13: See Hoffstein on col.10, lines 35-40 and Irvin on col.4, lines 30-46 and col.11, lines 10-12; discussing the parameter generation apparatus according to claim 10, wherein the provisional parameter generation unit generates the non-negative integer q included in the set of provisional parameters, based on the error condition information.

As per claim 14: See Hoffstein on col.5, lines 10-20 and col.10, lines 25-40; discussing the parameter generation apparatus according to claim 10, wherein the output parameter generation unit generates the degree N included in the output parameter, based on the security level information and the security determination information.

As per claim 17: See Hoffstein on col.6, lines 15-60 and col.12, lines 30-57; discussing the parameter generation apparatus according to claim 1, wherein the NTRU cryptosystem is an encryption system for encrypting a plain text and decrypting an encrypted text by a method comprising the following steps: a selection step of selecting ideals p and q of a ring R that is a group of arrays of dimension N in which addition, subtraction and multiplication are defined; a generation step of generating elements f and g of the ring R, and generating element F.sub.q which is an inverse of f (mod q), and generating element F.sub.p which is an inverse of f (mod p); a public key production step of producing a public key that includes h, where h is congruent, mod q, to a product that can be derived using g and F.sub.q; a private key production step of producing, as a private key, information from which f and Fsub.p can be derived; an encryption step of producing the encrypted text by encoding the plain text using the public key and element i that is randomly selected from the ring R; and a decryption step of producing a decrypted text by decrypting the encrypted text using the private key.

As per claim 18:

Hoffstein discloses an encryption system for generating an encrypted text by encrypting a plain text in compliance with an *NTRU cryptosystem*, the encryption system comprising:

a parameter generation apparatus that includes an error-free output parameter generation unit operable to generate an output parameter causing no decryption error based on error condition information that is provided in advance, the error condition information indicating a condition for causing no decryption error;

a public key generation unit operable to generate a public key based on the output parameter generated by the parameter generation apparatus; and **(col.4, lines 13-30)** an encryption unit operable to encrypt the plain text based on the public key, **(col.10, lines 55-67 and col.11, lines 1-15)**

wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and

wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial f whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem. (col.9, lines 44-67 and col.10, lines 25-52 and col.11, lines 10=-55)

Hoffstein, ET al. is inventors for NTRU Cryptosystems, Inc. Hoffstein discloses encoding and decoding of information, more particularly, a public key cryptosystem for encryption and decryption of digital messages by processor system (col.1, lines 15-19). The invention allows keys to be chosen essentially at random from a large set of vectors, with key lengths comparable to the key lengths in other common public key cryptosystems, and features an appropriate security level, and provides encoding and decoding processes which are between one and two orders of magnitude faster than the most widely used public cryptosystem, namely the exponentiation cryptosystem (col.2, lines 45-53). Hoffstein further discusses. The Hoffstein reference suggests (col.6-col.12) the current amendment "wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem", for the fifth type of trap door function which has been used to create public key cryptosystems is based on error correcting codes (col.2, lines 14-21).

However, did not further include generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error.

Irvine includes an error check value generation circuit based on the unencrypted message and adds the error check value to the encrypted message (col.6, lines 45-50). Irvine discloses generating an error check value for the decrypted message can determine if there is no error. The error check value for the decrypted message can indicate no error message (col.4, lines 30-46 and col.11, lines 10-12).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Hoffstein with Irvin to teach generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error because to selectively encrypt and decrypt messages transmitted on the communication network by generating error check value for the decrypted message indicates no error (Irvin - col.4, lines 30-46 and col.11, lines 10-12).

As per claim 19:

Hoffstein discloses a decryption system for generating a decrypted text by decrypting an encrypted text in compliance with an NTRU cryptosystem, the decryption system comprising:

a parameter generation apparatus that includes an error-free output parameter generation unit operable to generate an output parameter causing no decryption error *based on error condition information that is provided in advance, the error condition information indicating a condition for causing no decryption error;*

a private key generation unit operable to generate a private key based on the output parameter generated by the parameter generation apparatus; and **(col.10, lines 55-67 and col.11, lines 1-15)**

a decryption unit operable to decrypt the encrypted text based on the private key, **(col.11, lines 17-23)**

wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and

wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial f whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem. (col.9, lines 44-67 and col.10, lines 25-52 and col.11, lines 10-55)

Hoffstein, ET al. is inventors for NTRU Cryptosystems, Inc. Hoffstein discloses encoding and decoding of information, more particularly, a public key cryptosystem for encryption and decryption of digital messages by processor system (col.1, lines 15-19). The invention allows keys to be chosen essentially at random from a large set of vectors, with key lengths comparable to the key lengths in other common public key cryptosystems, and features an appropriate security level, and provides encoding and decoding processes which are between one and two orders of magnitude faster than the most widely used public cryptosystem, namely the exponentiation cryptosystem (col.2, lines 45-53). Hoffstein further discusses. The Hoffstein reference suggests (col.6-col.12) the current amendment "wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem", for the fifth type of trap door function which has been used to create public key cryptosystems is based on error correcting codes (col.2, lines 14-21).

However, did not further include generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error.

Irvine includes an error check value generation circuit based on the unencrypted message and adds the error check value to the encrypted message (col.6, lines 45-50). Irvine discloses generating an error check value for the decrypted message can determine if there is no error (col.4, lines 30-34 and col.7, lines 22-25). The error check value for the decrypted message can indicate no error message (col.4, lines 30-46 and col.11, lines 10-12).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Hoffstein with Irvin to teach generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error because to selectively encrypt and decrypt messages transmitted on the communication network by generating error check value for the decrypted message indicates no error (Irvin - col.4, lines 30-46 and col.11, lines 10-12).

As per claim 20:

Hoffstein discloses an encryption system using an NTRU cryptosystem, the encryption system comprising:

a parameter generation apparatus for generating and outputting an output parameter that is a set of parameters *causing no decryption error* for the NTRU cryptosystem;

a key generation apparatus for generating and outputting an encryption key and a decryption key for the NTRU cryptosystem; **(col.10, lines 55-67 and col.11, lines 1-15)** an encryption apparatus for generating an encrypted text by encrypting a plain text in compliance with the NTRU cryptosystem; and **(col.4, lines 13-30 and col.10, lines 30-35)**

a decryption apparatus for generating a decrypted text by decrypting the encrypted text, wherein the parameter generation apparatus includes: **(col.11, lines 17-23)**

a provisional parameter generation unit operable to generate a set of provisional parameters <u>causing no decryption error</u>*, based on error condition information that is provided in advance, the error condition information indicating a condition for causing no decryption error; and*

an output parameter generation unit operable to generate the output parameter, using the set of provisional parameters, based on a lattice constant that is calculated from the set of provisional parameters, and

<u>wherein</u> output the generated output parameter, the key generation apparatus includes a generated key output unit operable to generate the encryption key and the decryption key, using the output parameter inputted from the parameter generation apparatus, and output the generated encryption key and decryption key,

<u>wherein</u> the encryption apparatus includes an encryption unit operable to generate the encrypted text by encrypting the plain text, using the output parameter inputted from the parameter generation apparatus and the encryption key inputted from the key generation apparatus, and

wherein the decryption apparatus includes a decryption unit operable to generate the decrypted text by decrypting the encrypted text, using the output parameter inputted from the parameter generation apparatus and the decryption key inputted from the key generation apparatus, **(col.10, lines 35-40 and col.12, lines 10-55)**

wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and

wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial f whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem. (col.9, lines 44-67 and col.10, lines 25-52 and col.11, lines 10-55)

Hoffstein, ET al. is inventors for NTRU Cryptosystems, Inc. Hoffstein discloses encoding and decoding of information, more particularly, a public key cryptosystem for encryption and decryption of digital messages by processor system (col.1, lines 15-19). The invention allows keys to be chosen essentially at random from a large set of vectors, with key lengths comparable to the key lengths in other common public key cryptosystems, and features an appropriate security level, and provides encoding and decoding processes which are between one and two orders of magnitude faster than the most widely used public cryptosystem, namely the exponentiation cryptosystem (col.2, lines 45-53). Hoffstein further discusses. The Hoffstein reference suggests (col.6-col.12) the current amendment “wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and wherein the conditional expression is represented as $2 \cdot p \cdot d + 2df - 1\ q/2$, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem", for the fifth type of trap door function which has been used to create public key cryptosystems is based on error correcting codes (col.2, lines 14-21).

However, did not further include generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error.

Irvine includes an error check value generation circuit based on the unencrypted message and adds the error check value to the encrypted message (col.6, lines 45-50). Irvine discloses generating an error check value for the decrypted message can determine if there is no error (col.4, lines 30-34 and col.7, lines 22-25). The error check value for the decrypted message can indicate no error message (col.4, lines 30-46 and col.11, lines 10-12).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Hoffstein with Irvin to teach generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error because to selectively encrypt and decrypt messages transmitted on the communication network by generating error check value for the decrypted message indicates no error (Irvin - col.4, lines 30-46 and col.11, lines 10-12).

As per claim 21:

Hoffstein discloses an n encryption system using an NTRU cryptosystem, the encryption system comprising:

a parameter generation apparatus for generating and outputting an output parameter that is a set of parameters *causing no decryption error* for the NTRU cryptosystem; **(col.4, lines 13-30 and col.10, lines 25-50)**

a key generation apparatus for generating and outputting an encryption key for the NTRU cryptosystem; and **(col.10, lines 55-67 and col.11, lines 1-15)**

an encryption apparatus for generating an encrypted text by encrypting a plain text in compliance with the NTRU cryptosystem, wherein the parameter generation apparatus includes: **(col.11, lines 17-23)**

a provisional parameter generation unit operable to generate a set of provisional parameters causing no decryption error *based on error condition information that is provided in advance, the error condition information indicating a condition for causing no decryption error; and*

an output parameter generation unit operable to generate the output parameter, using the set of provisional parameters, based on a lattice constant that is calculated from the set of provisional parameters, and output the generated output parameter,

wherein the key generation apparatus includes a generated key output unit operable to generate the encryption key, using the output parameter inputted from the parameter generation apparatus, and output the generated encryption key, and

wherein the encryption apparatus includes an encryption unit operable to generate the encrypted text by encrypting the plain text, using the output parameter inputted from the parameter generation apparatus and

wherein the encryption key inputted from the key generation apparatus, **(col.10, lines 35-40 and col.12, lines 10-55)**

wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and

wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial f whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem. (col.9, lines 44-67 and col.10, lines 25-52 and col.11, lines 10-55)

Hoffstein, ET al. is inventors for NTRU Cryptosystems, Inc. Hoffstein discloses encoding and decoding of information, more particularly, a public key cryptosystem for encryption and decryption of digital messages by processor system (col.1, lines 15-19). The invention allows keys to be chosen essentially at random from a large set of vectors, with key lengths comparable to the key lengths in other common public key cryptosystems, and features an appropriate security level, and provides encoding and decoding processes which are between one and two orders of magnitude faster than the most widely used public cryptosystem, namely the exponentiation cryptosystem (col.2, lines 45-53). Hoffstein further discusses. The Hoffstein reference suggests (col.6-col.12) the current amendment “wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem”, for the fifth type of trap door function which has been used to create public key cryptosystems is based on error correcting codes (col.2, lines 14-21).

However, did not further include generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error.

Irvine includes an error check value generation circuit based on the unencrypted message and adds the error check value to the encrypted message (col.6, lines 45-50). Irvine discloses generating an error check value for the decrypted message can determine if there is no error (col.4, lines 30-34 and col.7, lines 22-25). The error check value for the decrypted message can indicate no error message (col.4, lines 30-46 and col.11, lines 10-12).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Hoffstein with Irvin to teach generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error because to selectively encrypt and decrypt messages transmitted on the communication network by generating error check value for the decrypted message indicates no error (Irvin - col.4, lines 30-46 and col.11, lines 10-12).

As per claim 22:

Hoffstein discloses an encryption apparatus for generating an encrypted text by encrypting a plain text in compliance with an NTRU cryptosystem, the encryption apparatus comprising:

a provisional parameter generation unit operable to generate a set of provisional parameters causing no decryption error *based on error condition information that is provided in advance, the error condition information indicating a condition for causing no decryption error;*

an output parameter generation unit operable to generate an output parameter, using the set of provisional parameters, based on a lattice constant that is calculated from the set of provisional parameters, and output the generated output parameter the output parameter being a set of parameters causing no decryption error for the NTRU cryptosystem; **(col.10, lines 35-40 and col.12, lines 10-55)**

a parameter transmission unit operable to transmit the output parameter to a decryption apparatus; **(col.4, lines 13-30 and col.5, lines 10-40)** an encryption key receiving unit operable to receive, from the decryption apparatus, an encryption key for the NTRU cryptosystem that is generated based on the output parameter; and **(col.10, lines 55-67 and col.11, lines 1-15)**

an encrypted text generation unit operable to generate the encrypted text by encrypting the plain text based on the output parameter and the encryption key, **(col.11, lines 10-23)**

wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and

wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial f whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem. (col.9, lines 44-67 and col.10, lines 25-52 and col.11, lines 10-55)

Hoffstein, ET al. is inventors for NTRU Cryptosystems, Inc. Hoffstein discloses encoding and decoding of information, more particularly, a public key cryptosystem for encryption and decryption of digital messages by processor system (col.1, lines 15-19). The invention allows keys to be chosen essentially at random from a large set of vectors, with key lengths comparable to the key lengths in other common public key cryptosystems, and features an appropriate security level, and provides encoding and decoding processes which are between one and two orders of magnitude faster than the most widely used public cryptosystem, namely the exponentiation cryptosystem (col.2, lines 45-53). Hoffstein further discusses. The Hoffstein reference suggests (col.6-col.12) the current amendment “wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem”, for the fifth type of trap door function which has been used to create public key cryptosystems is based on error correcting codes (col.2, lines 14-21).

However, did not further include generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error.

Irvine includes an error check value generation circuit based on the unencrypted message and adds the error check value to the encrypted message (col.6, lines 45-50). Irvine discloses generating an error check value for the decrypted message can determine if there is no error (col.4, lines 30-34 and col.7, lines 22-25). The error check value for the decrypted message can indicate no error message (col.4, lines 30-46 and col.11, lines 10-12).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Hoffstein with Irvin to teach generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error because to selectively encrypt and decrypt messages transmitted on the communication network by generating error check value for the decrypted message indicates no error (Irvin - col.4, lines 30-46 and col.11, lines 10-12).

As per claim 23:

Hoffstein discloses an encryption apparatus for generating an encrypted text by encrypting a plain text in compliance with an NTRU cryptosystem, the encryption apparatus comprising:

a parameter receiving unit operable to receive an output parameter causing no decryption error *and that is generated based on error condition information that is provided in advance, the error condition information indicating a condition for causing no decryption error;*

a public key generation unit operable to generate a public key based on the output parameter received by the parameter receiving unit; and **(col.4, lines 13-30 and col.5, lines 10-40)**

an encryption unit operable to encrypt the plain text based on the public key, **(col.10, lines 55-67 and col.11, lines 1-23)**

wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and

wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial f whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem. (col.9, lines 44-67 and col.10, lines 25-52 and col.11, lines 10-55)

Hoffstein, ET al. is inventors for NTRU Cryptosystems, Inc. Hoffstein discloses encoding and decoding of information, more particularly, a public key cryptosystem for encryption and decryption of digital messages by processor system (col.1, lines 15-19). The invention allows keys to be chosen essentially at random from a large set of vectors, with key lengths comparable to the key lengths in other common public key cryptosystems, and features an appropriate security level, and provides encoding and decoding processes which are between one and two orders of magnitude faster than the most widely used public cryptosystem, namely the exponentiation cryptosystem (col.2, lines 45-53). Hoffstein further discusses. The Hoffstein reference suggests (col.6-col.12) the current amendment "wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem", for the fifth type of trap door function which has been used to create public key cryptosystems is based on error correcting codes (col.2, lines 14-21).

However, did not further include generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error.

Irvine includes an error check value generation circuit based on the unencrypted message and adds the error check value to the encrypted message (col.6, lines 45-50). Irvine discloses generating an error check value for the decrypted message can determine if there is no error (col.4, lines 30-34 and col.7, lines 22-25). The error check value for the decrypted message can indicate no error message (col.4, lines 30-46 and col.11, lines 10-12).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Hoffstein with Irvin to teach generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error because to selectively encrypt and decrypt messages transmitted on the communication network by generating error check value for the decrypted message indicates no error (Irvin - col.4, lines 30-46 and col.11, lines 10-12).

As per claim 24:

Hoffstein discloses an n encryption method for generating an encrypted text by encrypting a plain text in compliance with NTRU cryptosystem, the encryption method comprising the steps of:

generating a set of provisional parameters causing no decryption error *based on error condition information that is provided in advance, the error condition information indicating a condition for causing no decryption error;*

generating an output parameter using the set of provisional parameters, based on a lattice constant that is calculated from the set of provisional parameters, and outputting the generated output parameter, the generated output parameter being a set of parameters causing no decryption error for the NTRU cryptosystem; **(col.4, lines 13-30 and col.10, lines 35-40 and col.12, lines 10-55)**

generating an encryption key for the NTRU cryptosystem based on the output parameter; and **(col.10, lines 55-67 and col.11, lines 1-15)**

generating the encrypted text by encrypting the plain text, based on the output parameter and the encryption key, **(col.11, lines 10-23)**

wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and

wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial f whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem. (col.9, lines 44-67 and col.10, lines 25-52 and col.11, lines 10-55)

Hoffstein, ET al. is inventors for NTRU Cryptosystems, Inc. Hoffstein discloses encoding and decoding of information, more particularly, a public key cryptosystem for encryption and decryption of digital messages by processor system (col.1, lines 15-19). The invention allows keys to be chosen essentially at random from a large set of vectors, with key lengths comparable to the key lengths in other common public key cryptosystems, and features an appropriate security level, and provides encoding and decoding processes which are between one and two orders of magnitude faster than the most widely used public cryptosystem, namely the exponentiation cryptosystem (col.2, lines 45-53). Hoffstein further discusses. The Hoffstein reference suggests (col.6-col.12) the current amendment “wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and wherein the conditional expression is represented as $2 \cdot p \cdot d + 2df- 1\ q/2$, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem”, for the fifth type of trap door function which has been used to create public key cryptosystems is based on error correcting codes (col.2, lines 14-21).

However, did not further include generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error.

Irvine includes an error check value generation circuit based on the unencrypted message and adds the error check value to the encrypted message (col.6, lines 45-50). Irvine discloses generating an error check value for the decrypted message can determine if there is no error (col.4, lines 30-34 and col.7, lines 22-25). The error check value for the decrypted message can indicate no error message (col.4, lines 30-46 and col.11, lines 10-12).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Hoffstein with Irvin to teach generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error because to selectively encrypt and decrypt messages transmitted on the communication network by generating error check value for the decrypted message indicates no error (Irvin- col.4, lines 30-46 and col.11, lines 10-12).

As per claim 25:

Hoffstein discloses a non-transitory computer-readable recording medium having stored therein a program for generating an encrypted text by encrypting a plain text in compliance with NTRU cryptosystem, wherein when executed the program causes a computer to perform a method comprising the steps of:

generating a set of provisional parameters causing no decryption error *condition information that is provided in advance, the error condition information indicating a condition for causing no decryption error;*

generating an output parameter using the set of provisional parameters, based on a lattice constant that is calculated from the set of provisional parameters, and outputting the generated output parameter, the generated output parameter being a set of parameters causing no decryption error for the NTRU cryptosystem; **(col.4, lines 13-30 and col.10, lines 35-40 and col.12, lines 10-55)**

generating an encryption key for the NTRU cryptosystem based on the output parameter; and **(col.10, lines 55-67 and col.11, lines 1-15)**

generating the encrypted text by encrypting the plain text, based on the output parameter and the encryption key, **(col.11, lines 10-23)**

wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and

wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial f whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem. (col.9, lines 44-67 and col.10, lines 25-52 and col.11, lines 10-55)

Hoffstein, ET al. is inventors for NTRU Cryptosystems, Inc. Hoffstein discloses encoding and decoding of information, more particularly, a public key cryptosystem for encryption and decryption of digital messages by processor system (col.1, lines 15-19). The invention allows keys to be chosen essentially at random from a large set of vectors, with key lengths comparable to the key lengths in other common public key cryptosystems, and features an appropriate security level, and provides encoding and decoding processes which are between one and two orders of magnitude faster than the most widely used public cryptosystem, namely the exponentiation cryptosystem (col.2, lines 45-53). Hoffstein further discusses. The Hoffstein reference suggests (col.6-col.12) the current amendment “wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and wherein the conditional expression is represented as $2 \cdot p \cdot d + 2df- 1 \; q/2$, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem”, for the fifth type of trap door function which has been used to create public key cryptosystems is based on error correcting codes (col.2, lines 14-21).

However, did not further include generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error.

Irvine includes an error check value generation circuit based on the unencrypted message and adds the error check value to the encrypted message (col.6, lines 45-50). Irvine discloses generating an error check value for the decrypted message can determine if there is no error (col.4, lines 30-34 and col.7, lines 22-25). The error check value for the decrypted message can indicate no error message (col.4, lines 30-46 and col.11, lines 10-12).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Hoffstein with Irvin to teach generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error because to selectively encrypt and decrypt messages transmitted on the communication network by generating error check value for the decrypted message indicates no error (Irvin- col.4, lines 30-46 and col.11, lines 10-12).

As per claim 26:

Hoffstein discloses a decryption system using an NTRU cryptosystem, the decryption system comprising:

a parameter generation apparatus for generating and outputting an output parameter that is a set of parameters *causing no decryption error* for the NTRU cryptosystem; **(col.4, lines 13-30 and col.5, lines 10-40)**

a key generation apparatus for generating and outputting a decryption key for the NTRU cryptosystem; and **(col.10, lines 55-67 and col.11, lines 1-15)**

a decryption apparatus for generating a decrypted text by decrypting an encrypted text in compliance with the NTRU cryptosystem, wherein the parameter generation apparatus includes: **(col.11, lines 17-23)**

a provisional parameter generation unit operable to generate a set of provisional parameters causing no decryption error *based on error condition information that is provided in advance the error condition information indicating a condition for causing no decryption error; and*

an output parameter generation unit operable to generate the output parameter, using the set of provisional parameters, based on a lattice constant that is calculated from the set of provisional parameters, and output the generated output parameter,

the key generation apparatus includes a generated key output unit operable to generate the decryption key, using the output parameter inputted from the parameter generation apparatus, and output the generated decryption key, and

the decryption apparatus includes a decryption unit operable to generate the decrypted text by decrypting the encrypted text, using the output parameter inputted from the parameter generation apparatus and the decryption key inputted from the key generation apparatus, **(col.10, lines 35-40 and col.12, lines 10-55)**

wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and

wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial f whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem. (col.9, lines 44-67 and col.10, lines 25-52 and col.11, lines 10-55)

Hoffstein, ET al. is inventors for NTRU Cryptosystems, Inc. Hoffstein discloses encoding and decoding of information, more particularly, a public key cryptosystem for encryption and decryption of digital messages by processor system (col.1, lines 15-19). The invention allows keys to be chosen essentially at random from a large set of vectors, with key lengths comparable to the key lengths in other common public key cryptosystems, and features an appropriate security level, and provides encoding and decoding processes which are between one and two orders of magnitude faster than the most widely used public cryptosystem, namely the exponentiation cryptosystem (col.2, lines 45-53). Hoffstein further discusses. The Hoffstein reference suggests (col.6-col.12) the current amendment "wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem", for the fifth type of trap door function which has been used to create public key cryptosystems is based on error correcting codes (col.2, lines 14-21).

However, did not further include generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error.

As per claim 27:

Hoffstein discloses a decryption apparatus for generating a decrypted text by decrypting an encrypted text received from an encryption apparatus in compliance with an NTRU cryptosystem, the decryption apparatus comprising:

a parameter receiving unit operable to receive, from the encryption apparatus, an output parameter, the output parameter being *a set of parameters causing no decryption error for the NTRU cryptosystem;*

a generated key generation unit operable to generate an encryption key and a decryption key for the NTRU cryptosystem, using the inputted output parameter, and output the generated encryption key and decryption key; **(col.4, lines 10-30 and col.12, lines 10-55)**

an encryption key transmission unit operable to transmit the encrypted key to the encryption apparatus; and **(col.10, lines 55-67 and col.11, lines 1-15)**

a decrypted text generation unit operable to generate the decrypted text by decrypting the encrypted text based on the output parameter and the decryption key, **(col.11, lines 17-23)**

wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and

wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial f whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem. (col.9, lines 44-67 and col.10, lines 25-52 and col.11, lines 10-55)

Hoffstein, ET al. is inventors for NTRU Cryptosystems, Inc. Hoffstein discloses encoding and decoding of information, more particularly, a public key cryptosystem for encryption and decryption of digital messages by processor system (col.1, lines 15-19). The invention allows keys to be chosen essentially at random from a large set of vectors, with key lengths comparable to the key lengths in other common public key cryptosystems, and features an appropriate security level, and provides encoding and decoding processes which are between one and two orders of magnitude faster than the most widely used public cryptosystem, namely the exponentiation cryptosystem (col.2, lines 45-53). Hoffstein further discusses. The Hoffstein reference suggests (col.6-col.12) the current amendment "wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem", for the fifth type of trap door function which has been used to create public key cryptosystems is based on error correcting codes (col.2, lines 14-21).

However, did not further include generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error.

Irvine includes an error check value generation circuit based on the unencrypted message and adds the error check value to the encrypted message (col.6, lines 45-50). Irvine discloses generating an error check value for the decrypted message can determine if there is no error (col.4, lines 30-34 and col.7, lines 22-25). The error check value for the decrypted message can indicate no error message (col.4, lines 30-46 and col.11, lines 10-12).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Hoffstein with Irvin to teach generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error because to selectively encrypt and decrypt messages transmitted on the communication network by generating error check value for the decrypted message indicates no error (Irvin- col.4, lines 30-46 and col.11, lines 10-12).

As per claim 28:

Hoffstein discloses a decryption method for generating a decrypted text by decrypting an encrypted text in compliance with NTRU cryptosystem, the decryption method comprising the steps of:

generating a set of provisional parameters causing no decryption error *based on error condition information that is provided in advance, the error condition information indicating a condition for causing no decryption error;*

generating an output parameter using the set of provisional parameters, based on a lattice constant that is calculated from the set of provisional parameters, and outputting the generated output parameter, the generated output parameter being a set of parameters causing no decryption error for the NTRU cryptosystem; **(col.4, lines 13-30 and col.10, lines 35-40 and col.12, lines 10-55)**

generating a decryption key for the NTRU cryptosystem based on the output parameter; and **(col.10, lines 55-67 and col.11, lines 1-15)** generating the decrypted text by decrypting the encrypted text, based on the output parameter and the decryption key, **(col.11, lines 17-23)**

wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and

wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial f whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem. (col.9, lines 44-67 and col.10, lines 25-52 and col.11, lines 10-55)

Hoffstein, ET al. is inventors for NTRU Cryptosystems, Inc. Hoffstein discloses encoding and decoding of information, more particularly, a public key cryptosystem for encryption and decryption of digital messages by processor system (col.1, lines 15-19). The invention allows keys to be chosen essentially at random from a large set of vectors, with key lengths comparable to the key lengths in other common public key cryptosystems, and features an appropriate security level, and provides encoding and decoding processes which are between one and two orders of magnitude faster than the most widely used public cryptosystem, namely the exponentiation cryptosystem (col.2, lines 45-53). Hoffstein further discusses. The Hoffstein reference suggests (col.6-col.12) the current amendment "wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem", for the fifth type of trap door function which has been used to create public key cryptosystems is based on error correcting codes (col.2, lines 14-21).

However, did not further include generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error.

Irvine includes an error check value generation circuit based on the unencrypted message and adds the error check value to the encrypted message (col.6, lines 45-50). Irvine discloses generating an error check value for the decrypted message can determine if there is no error (col.4, lines 30-34 and col.7, lines 22-25). The error check value for the decrypted message can indicate no error message (col.4, lines 30-46 and col.11, lines 10-12).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Hoffstein with Irvin to teach generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error because to selectively encrypt and decrypt messages transmitted on the communication network by generating error check value for the decrypted message indicates no error (Irvin- col.4, lines 30-46 and col.11, lines 10-12).

As per claim 29:

Hoffstein discloses a non-transitory computer-readable recording medium having stored therein a program for generating an encrypted text by encrypting a plain text in compliance with NTRU cryptosystem, wherein when executed the program causes a computer to perform a method comprising the steps of:

generating a set of provisional parameters *the output parameter being* causing no decryption error based on error condition information that is provided in advance, the error condition information indicating a condition for causing no decryption error;

generating an output parameter using the set of provisional parameters, based on a lattice constant that is calculated from the set of provisional parameters, and outputting the generated output parameter, the generated output parameter being a set of parameters causing no decryption error for the NTRU cryptosystem; **(col.4, lines 13-30 and col.10, lines 35-40 and col.12, lines 10-55)**

generating a decryption key for the NTRU cryptosystem based on the output parameter; and **(col.10, lines 55-67 and col.11, lines 1-15)**

generating the decrypted text by decrypting the encrypted text based on the output parameter and the decryption key, **(col.11, lines 10-23)**

wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and

wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial f whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem. (col.9, lines 44-67 and col.10, lines 25-52 and col.11, lines 10-55)

Hoffstein, ET al. is inventors for NTRU Cryptosystems, Inc. Hoffstein discloses encoding and decoding of information, more particularly, a public key cryptosystem for encryption and decryption of digital messages by processor system (col.1, lines 15-19). The invention allows keys to be chosen essentially at random from a large set of vectors, with key lengths comparable to the key lengths in other common public key cryptosystems, and features an appropriate security level, and provides encoding and decoding processes which are between one and two orders of magnitude faster than the most widely used public cryptosystem, namely the exponentiation cryptosystem (col.2, lines 45-53). Hoffstein further discusses. The Hoffstein reference suggests (col.6-col.12) the current amendment “wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem”, for the fifth type of trap door function which has been used to create public key cryptosystems is based on error correcting codes (col.2, lines 14-21).

However, did not further include generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error.

Irvine includes an error check value generation circuit based on the unencrypted message and adds the error check value to the encrypted message (col.6, lines 45-50). Irvine discloses generating an error check value for the decrypted message can determine if there is no error (col.4, lines 30-34 and col.7, lines 22-25). The error check value for the decrypted message can indicate no error message (col.4, lines 30-46 and col.11, lines 10-12).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Hoffstein with Irvin to teach generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error because to selectively encrypt and decrypt messages transmitted on the communication network by generating error check value for the decrypted message indicates no error (Irvin- col.4, lines 30-46 and col.11, lines 10-12).

As per claim 30:

Hoffstein discloses an encryption system using an NTRU cryptosystem, the encryption system comprising:

a parameter conversion apparatus for converting, into an output parameter, an input parameter that is a set of parameters for the NTRU cryptosystem that are inputted from outside, the output parameter being a set of parameters causing no decryption error for the NTRU cryptosystem;

a key generation apparatus for generating and outputting an encryption key and a decryption key for the NTRU cryptosystem; **(col.4, lines 13-30 and col.5, lines 10-40)**

an encryption apparatus for generating an encrypted text by encrypting a plain text in compliance with the NTRU cryptosystem; and **(col.10, lines 55-67 and col.11, lines 1-15)**

a decryption apparatus for generating a decrypted text by decrypting the encrypted text, wherein the parameter conversion apparatus includes: **(col.10, lines 17-23)**

a provisional parameter generation unit operable to generate a set of provisional parameters that do not cause any decryption errors, based on the input parameter and error condition information that is provided in advance, the error condition information indicating a condition for causing no decryption error; and

an output parameter generation unit operable to generate the output parameter, using the set of provisional parameters, based on a lattice constant that is calculated from the set of provisional parameters, and output the generated output parameter, the key generation apparatus includes a generated key output unit operable to generate the encryption key and the decryption key, using the output parameter inputted from the parameter conversion apparatus, and output the generated encryption key and decryption key, the encryption apparatus includes an encryption unit operable to generate the encrypted text by encrypting the plain text, using the output parameter inputted from the parameter conversion apparatus and the encryption key inputted from the key generation apparatus, and the decryption apparatus includes a decryption unit operable to generate the decrypted text by decrypting the encrypted text, using the output parameter inputted from the parameter conversion apparatus and the decryption key inputted from the key generation apparatus, **(col.10, lines 35-40 and col.12, lines 10-55)**

wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and

wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial f whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem. (col.9, lines 44-67 and col.10, lines 25-52 and col.11, lines 10-55)

Hoffstein, ET al. is inventors for NTRU Cryptosystems, Inc. Hoffstein discloses encoding and decoding of information, more particularly, a public key cryptosystem for encryption and decryption of digital messages by processor system (col.1, lines 15-19). The invention allows keys to be chosen essentially at random from a large set of vectors, with key lengths comparable to the key lengths in other common public key cryptosystems, and features an appropriate security level, and provides encoding and decoding processes which are between one and two orders of magnitude faster than the most widely used public cryptosystem, namely the exponentiation cryptosystem (col.2, lines 45-53). Hoffstein further discusses. The Hoffstein reference suggests (col.6-col.12) the current amendment "wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and wherein the conditional expression is represented as $2 \bullet p \bullet d + 2df- 1\ q/2$, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem", for the fifth type of trap door function which has been used to create public key cryptosystems is based on error correcting codes (col.2, lines 14-21).

However, did not further include generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error.

Irvine includes an error check value generation circuit based on the unencrypted message and adds the error check value to the encrypted message (col.6, lines 45-50). Irvine discloses generating an error check value for the decrypted message can determine if there is no error (col.4, lines 30-34 and col.7, lines 22-25). The error check value for the decrypted message can indicate no error message (col.4, lines 30-46 and col.11, lines 10-12).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Hoffstein with Irvin to teach generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error because to selectively encrypt and decrypt messages transmitted on the communication network by generating error check value for the decrypted message indicates no error (Irvin- col.4, lines 30-46 and col.11, lines 10-12).

As per claim 31:

Hoffstein discloses an encryption system using an NTRU cryptosystem, the encryption system comprising:

a parameter generation apparatus for generating an output parameter from an input parameter that is a set of parameters for the NTRU cryptosystem that are inputted from outside, and outputting the generated output parameter that is a set of parameters causing no decryption error for the NTRU cryptosystem; **(col.4, lines 13-30 and col.5, lines 10-40)**

a key generation apparatus for generating and outputting an encryption key for the NTRU cryptosystem; and **(col.10, lines 55-67 and col.11, lines 1-15)**

an encryption apparatus for generating an encrypted text by encrypting a plain text in compliance with the NTRU cryptosystem, wherein the parameter generation apparatus includes: **(col.11, lines 10-23)**

a provisional parameter generation unit operable to generate a set of provisional parameters that do not cause any decryption errors, based on the input parameter and error condition information that is provided in advance, the error condition information indicating a condition for causing no decryption error; and

an output parameter generation unit operable to generate the output parameter, using the set of provisional parameters, based on a lattice constant that is calculated from the set of provisional parameters, and output the generated output parameter,

wherein the key generation apparatus includes a generated key output unit operable to generate the encryption key, using the output parameter inputted from the parameter generation apparatus, and output the generated encryption key, and

wherein the encryption apparatus includes an encryption unit operable to generate the encrypted text by encrypting the plain text, using the output parameter inputted from the parameter generation apparatus and the encryption key inputted from the key generation apparatus, **(col.10, lines 35-40 and col.12, lines 10-55)**

wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and

wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial f whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem. (col.9, lines 44-67 and col.10, lines 25-52 and col.11, lines 10-55)

Hoffstein, ET al. is inventors for NTRU Cryptosystems, Inc. Hoffstein discloses encoding and decoding of information, more particularly, a public key cryptosystem for encryption and decryption of digital messages by processor system (col.1, lines 15-19). The invention allows keys to be chosen essentially at random from a large set of vectors, with key lengths comparable to the key lengths in other common public key cryptosystems, and features an appropriate security level, and provides encoding and decoding processes which are between one and two orders of magnitude faster than the most widely used public cryptosystem, namely the exponentiation cryptosystem (col.2, lines 45-53). Hoffstein further discusses. The Hoffstein reference suggests (col.6-col.12) the current amendment “wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem”, for the fifth type of trap door function which has been used to create public key cryptosystems is based on error correcting codes (col.2, lines 14-21).

However, did not further include generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error.

Irvine includes an error check value generation circuit based on the unencrypted message and adds the error check value to the encrypted message (col.6, lines 45-50). Irvine discloses generating an error check value for the decrypted message can determine if there is no error (col.4, lines 30-34 and col.7, lines 22-25). The error check

value for the decrypted message can indicate no error message (col.4, lines 30-46 and col.11, lines 10-12).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Hoffstein with Irvin to teach generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error because to selectively encrypt and decrypt messages transmitted on the communication network by generating error check value for the decrypted message indicates no error (Irvin- col.4, lines 30-46 and col.11, lines 10-12).

As per claim 32:

Hoffstein discloses an n encryption apparatus for generating an encrypted text by encrypting a plain text in compliance with an NTRU cryptosystem, the encryption apparatus comprising:

a provisional parameter generation unit operable to generate a set of provisional parameters causing no decryption error *based on an input parameter that is a set of parameters for the NTRU cryptosystem and error condition information indicating a condition for causing no decryption error, the input parameter and error condition information being provided in advance*;

an output parameter generation unit operable to generate an output parameter, using the set of provisional parameters, based on a lattice constant that is calculated from the set of provisional parameters, and output the generated output parameter, the generated output parameter being a set of parameters causing no decryption error for the NTRU cryptosystem; **(col.10, lines 35-40 and col.12, lines 10-55)**

a parameter transmission unit operable to transmit the output parameter to a decryption apparatus; **(col.4, lines 13-30 and col.5, lines 10-40)**

an encryption key receiving unit operable to receive, from the decryption apparatus, an encryption key for the NTRU cryptosystem that is generated based on the output parameter; and **(col.10, lines 55-67 and col.11, lines 1-15)**

an encrypted text generation unit operable to generate the encrypted text by encrypting the plain text based on the output parameter and the encryption key, **(col.11, lines 10-23)**

wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and

wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial f whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem. (col.9, lines 44-67 and col.10, lines 25-52 and col.11, lines 10-55)

Hoffstein, ET al. is inventors for NTRU Cryptosystems, Inc. Hoffstein discloses encoding and decoding of information, more particularly, a public key cryptosystem for encryption and decryption of digital messages by processor system (col.1, lines 15-19). The invention allows keys to be chosen essentially at random from a large set of vectors, with key lengths comparable to the key lengths in other common public key cryptosystems, and features an appropriate security level, and provides encoding and decoding processes which are between one and two orders of magnitude faster than the most widely used public cryptosystem, namely the exponentiation cryptosystem (col.2, lines 45-53). Hoffstein further discusses. The Hoffstein reference suggests (col.6-col.12) the current amendment "wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem", for the fifth type of trap door function which has been used to create public key cryptosystems is based on error correcting codes (col.2, lines 14-21).

However, did not further include generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error.

Irvine includes an error check value generation circuit based on the unencrypted message and adds the error check value to the encrypted message (col.6, lines 45-50). Irvine discloses generating an error check value for the decrypted message can determine if there is no error (col.4, lines 30-34 and col.7, lines 22-25). The error check

value for the decrypted message can indicate no error message (col.4, lines 30-46 and col.11, lines 10-12).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Hoffstein with Irvin to teach generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error because to selectively encrypt and decrypt messages transmitted on the communication network by generating error check value for the decrypted message indicates no error (Irvin- col.4, lines 30-46 and col.11, lines 10-12).

As per claim 33:

Hoffstein discloses an encryption method for generating an encrypted text by encrypting a plain text in compliance with NTRU cryptosystem, the encryption method comprising the following steps of:

generating a set of provisional parameters causing no decryption error *based on an input parameter that is a set of parameters for the NTRU cryptosystem and error condition information indicating a condition for causing no decryption error, the input parameter and error condition information being provided in advance;*

generating an output parameter using the set of provisional parameters, based on a lattice constant that is calculated from the set of provisional parameters, and outputting the generated output parameter, the generated output parameter being a set of parameters causing no decryption error for the NTRU cryptosystem; **(col.4, lines 13-30 and col.10, lines 35-40 and col.12, lines 10-55)**

generating an encryption key for the NTRU cryptosystem based on the output parameter; and **(col.10, lines 55-67 and col.11, lines 1-15)**

generating the encrypted text by encrypting the plain text, based on the output parameter and the encryption key, **(col.11, lines 10-23)**

wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and

wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial f whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem.

Hoffstein, ET al. is inventors for NTRU Cryptosystems, Inc. Hoffstein discloses encoding and decoding of information, more particularly, a public key cryptosystem for encryption and decryption of digital messages by processor system (col.1, lines 15-19). The invention allows keys to be chosen essentially at random from a large set of vectors, with key lengths comparable to the key lengths in other common public key cryptosystems, and features an appropriate security level, and provides encoding and decoding processes which are between one and two orders of magnitude faster than the most widely used public cryptosystem, namely the exponentiation cryptosystem (col.2, lines 45-53). Hoffstein further discusses the fifth type of trap door function which has been used to create public key cryptosystems is based on error correcting codes (col.2, lines 14-21). However, did not further include generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error.

Irvine includes an error check value generation circuit based on the unencrypted message and adds the error check value to the encrypted message (col.6, lines 45-50). Irvine discloses generating an error check value for the decrypted message can determine if there is no error (col.4, lines 30-34 and col.7, lines 22-25). The error check value for the decrypted message can indicate no error message (col.4, lines 30-46 and col.11, lines 10-12).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Hoffstein with Irvin to teach generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error because to selectively encrypt and decrypt messages transmitted on the communication network by generating error check value for the decrypted message indicates no error (Irvin- col.4, lines 30-46 and col.11, lines 10-12).

<u>As per claim 34:</u>

Hoffstein discloses a <u>non-transitory computer-readable recording medium having stored therein a</u> program for generating an encrypted text by encrypting a plain text in compliance with NTRU cryptosystem, <u>wherein when executed,</u> the program <u>causes</u> a computer to <u>perform a method comprising the</u> steps of:

generating a set of provisional parameters <u>causing no decryption error</u> *based on an input parameter that is a set of parameters for the NTRU cryptosystem and error* *condition information indicating a condition for causing no decryption error, the input parameter and error condition information being provided in advance;*

generating an output parameter using the set of provisional parameters, based on a lattice constant that is calculated from the set of provisional parameters, and outputting the generated output parameter, the generated output parameter being a set of parameters causing no decryption error for the NTRU cryptosystem; **(col.4, lines 13-30 and col.10, lines 35-40 and col.12, lines 10-55)**

generating an encryption key for the NTRU cryptosystem based on the output parameter; and **(col.10, lines 55-67 and col.11, lines 1-15)**

generating the encrypted text by encrypting the plain text, based on the output parameter and the encryption key, **(col.11, lines 10-23)**

wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and

wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial f whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem. (col.9, lines 44-67 and col.10, lines 25-52 and col.11, lines 10-55)

Hoffstein, ET al. is inventors for NTRU Cryptosystems, Inc. Hoffstein discloses encoding and decoding of information, more particularly, a public key cryptosystem for encryption and decryption of digital messages by processor system (col.1, lines 15-19).

The invention allows keys to be chosen essentially at random from a large set of vectors, with key lengths comparable to the key lengths in other common public key cryptosystems, and features an appropriate security level, and provides encoding and decoding processes which are between one and two orders of magnitude faster than the most widely used public cryptosystem, namely the exponentiation cryptosystem (col.2, lines 45-53). Hoffstein further discusses. The Hoffstein reference suggests (col.6-col.12) the current amendment "wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem", for the fifth type of trap door function which has been used to create public key cryptosystems is based on error correcting codes (col.2, lines 14-21).

However, did not further include generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error.

Irvine includes an error check value generation circuit based on the unencrypted message and adds the error check value to the encrypted message (col.6, lines 45-50). Irvine discloses generating an error check value for the decrypted message can determine if there is no error (col.4, lines 30-34 and col.7, lines 22-25). The error check

value for the decrypted message can indicate no error message (col.4, lines 30-46 and col.11, lines 10-12).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Hoffstein with Irvin to teach generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error because to selectively encrypt and decrypt messages transmitted on the communication network by generating error check value for the decrypted message indicates no error (Irvin- col.4, lines 30-46 and col.11, lines 10-12).

As per claim 35:

Hoffstein discloses a decryption system using an NTRU cryptosystem, comprising:

a parameter generation apparatus for generating an output parameter from an input parameter that is a set of parameters for the NTRU cryptosystem that are inputted from outside, and outputting the generated output parameter, the generated output parameter being a set of parameters *causing no decryption error* for the NTRU cryptosystem; **(col.4, lines 13-30 and col.5, lines 10-40)**

a key generation apparatus for generating and outputting a decryption key for the NTRU cryptosystem; and **(col.10, lines 55-67 and col.11, lines 1-15)**

a decryption apparatus for generating a decrypted text by decrypting an encrypted text in compliance with the NTRU cryptosystem, wherein the parameter generation apparatus includes: **(col.11, lines 17-23)** *a provisional parameter generation unit operable to generate a set of provisional parameters* causing no decryption error *based on the input parameter and error condition information that is provided in advance, the error condition information indicating a condition for causing no decryption error; and*

an output parameter generation unit operable to generate the output parameter, using the set of provisional parameters, based on a lattice constant that is calculated from the set of provisional parameters, and output the generated output parameter,

wherein the key generation apparatus includes a generated key output unit operable to generate the decryption key, using the output parameter inputted from the parameter generation apparatus, and output the generated decryption key, and

wherein the decryption apparatus includes a decryption unit operable to generate the decrypted text by decrypting the encrypted text, using the output parameter inputted from the parameter generation apparatus and the decryption key inputted from the key generation apparatus, **(col.10, lines 35-40 and col.12, lines 10-55)**

wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and

wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial f whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem. (col.9, lines 44-67 and col.10, lines 25-52 and col.11, lines 10-55)

Hoffstein, ET al. is inventors for NTRU Cryptosystems, Inc. Hoffstein discloses encoding and decoding of information, more particularly, a public key cryptosystem for encryption and decryption of digital messages by processor system (col.1, lines 15-19). The invention allows keys to be chosen essentially at random from a large set of vectors, with key lengths comparable to the key lengths in other common public key cryptosystems, and features an appropriate security level, and provides encoding and decoding processes which are between one and two orders of magnitude faster than the most widely used public cryptosystem, namely the exponentiation cryptosystem (col.2, lines 45-53). Hoffstein further discusses. The Hoffstein reference suggests (col.6-col.12) the current amendment "wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem", for the fifth type of trap door function which has been used to create public key cryptosystems is based on error correcting codes (col.2, lines 14-21).

However, did not further include generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error.

Irvine includes an error check value generation circuit based on the unencrypted message and adds the error check value to the encrypted message (col.6, lines 45-50). Irvine discloses generating an error check value for the decrypted message can determine if there is no error (col.4, lines 30-34 and col.7, lines 22-25). The error check value for the decrypted message can indicate no error message (col.4, lines 30-46 and col.11, lines 10-12).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Hoffstein with Irvin to teach generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error because to selectively encrypt and decrypt messages transmitted on the communication network by generating error check value for the decrypted message indicates no error (Irvin- col.4, lines 30-46 and col.11, lines 10-12).

<u>As per claim 36:</u>

Hoffstein discloses a decryption method for generating a decrypted text by decrypting an encrypted text in compliance with NTRU cryptosystem, the decryption method comprising the following steps of:

generating a set of provisional parameters <u>causing no decryption error</u> *based on an input parameter that is a set of parameters for the NTRU cryptosystem and error condition information indicating a condition for causing no decryption error, the input parameter and error condition information being provided in advance;*

generating an output parameter using the set of provisional parameters, based on a lattice constant that is calculated from the set of provisional parameters, and outputting the generated output parameter, the generated output parameter being a set of parameters causing no decryption error for the NTRU cryptosystem; **(col.4, lines 13-30 and col.10, lines 35-40 and col.12, lines 10-55)**

generating a decryption key for the NTRU cryptosystem based on the output parameter; and **(col.10, lines 55-67 and col.11, lines 1-15)**

generating the decrypted text by decrypting the encrypted text, based on the output parameter and the decryption key, **(col.11, lines 17-23)**

wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and

wherein the conditional expression is represented as $2 \cdot p \cdot d + 2df- 1 q/2$, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial f whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem. (col.9, lines 44-67 and col.10, lines 25-52 and col.11, lines 10-55)

Hoffstein, ET al. is inventors for NTRU Cryptosystems, Inc. Hoffstein discloses encoding and decoding of information, more particularly, a public key cryptosystem for encryption and decryption of digital messages by processor system (col.1, lines 15-19). The invention allows keys to be chosen essentially at random from a large set of vectors, with key lengths comparable to the key lengths in other common public key cryptosystems, and features an appropriate security level, and provides encoding and decoding processes which are between one and two orders of magnitude faster than the most widely used public cryptosystem, namely the exponentiation cryptosystem (col.2, lines 45-53). Hoffstein further discusses. The Hoffstein reference suggests (col.6-col.12) the current amendment “wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem”, for the fifth type of trap door function which has been used to create public key cryptosystems is based on error correcting codes (col.2, lines 14-21).

However, did not further include generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error.

Irvine includes an error check value generation circuit based on the unencrypted message and adds the error check value to the encrypted message (col.6, lines 45-50). Irvine discloses generating an error check value for the decrypted message can determine if there is no error (col.4, lines 30-34 and col.7, lines 22-25). The error check value for the decrypted message can indicate no error message (col.4, lines 30-46 and col.11, lines 10-12).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Hoffstein with Irvin to teach generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error because to selectively encrypt and decrypt messages transmitted on the communication network by generating error check value for the decrypted message indicates no error (Irvin- col.4, lines 30-46 and col.11, lines 10-12).

As per claim 37:

Hoffstein discloses a non-transitory computer-readable recording medium having stored therein a program for generating an encrypted text by encrypting a plain text in compliance with NTRU cryptosystem, wherein when executed the program causes a computer to perform a method comprising the steps of:

generating a set of provisional parameters causing no decryption error *based on an input parameter that is a set of parameters for the NTRU cryptosystem and error condition information indicating a condition for causing no decryption error, the input parameter and error condition information being provided in advance;*

generating an output parameter using the set of provisional parameters, based on a lattice constant that is calculated from the set of provisional parameters, and outputting the generated output parameter, the generated output parameter being a set of parameters causing no decryption error for the NTRU cryptosystem; **(col.4, lines 13-30 and col.10, lines 35-40 and col.12, lines 10-55)**

generating a decryption key for the NTRU cryptosystem based on the output parameter; and **(col.10, lines 55-67 and col.11, lines 1-15)**

generating the decrypted text by decrypting the encrypted text, based on the output parameter and the decryption key, **(col.11, lines 17-23)**

wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and

wherein the conditional expression is represented as $2 \cdot p \cdot d + 2df- 1\ q/2$, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial f whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem. (col.9, lines 44-67 and col.10, lines 25-52 and col.11, lines 10-55)

Hoffstein, ET al. is inventors for NTRU Cryptosystems, Inc. Hoffstein discloses encoding and decoding of information, more particularly, a public key cryptosystem for encryption and decryption of digital messages by processor system (col.1, lines 15-19). The invention allows keys to be chosen essentially at random from a large set of vectors, with key lengths comparable to the key lengths in other common public key cryptosystems, and features an appropriate security level, and provides encoding and decoding processes which are between one and two orders of magnitude faster than the most widely used public cryptosystem, namely the exponentiation cryptosystem (col.2, lines 45-53). Hoffstein further discusses. The Hoffstein reference suggests (col.6-col.12) the current amendment “wherein the error condition information is a conditional expression indicating the condition for causing no decryption error, and wherein the conditional expression is represented as 2 • p • d + 2df- 1 q/2, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non- negative integer df, the non-negative integer df specifying the number of coefficients in a private key polynomial whose coefficient values equal to 1, and the non-negative integers being parameters for use in the NTRU cryptosystem", for the fifth type of trap door function which has been used to create public key cryptosystems is based on error correcting codes (col.2, lines 14-21).

However, did not further include generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error.

Irvine includes an error check value generation circuit based on the unencrypted message and adds the error check value to the encrypted message (col.6, lines 45-50). Irvine discloses generating an error check value for the decrypted message can determine if there is no error (col.4, lines 30-34 and col.7, lines 22-25). The error check value for the decrypted message can indicate no error message (col.4, lines 30-46 and col.11, lines 10-12).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Hoffstein with Irvin to teach generating output parameter that does not cause any decryption errors based on error condition information indicating a condition for causing no decryption error because to selectively encrypt and decrypt messages transmitted on the communication network by generating error check value for the decrypted message indicates no error (Irvin- col.4, lines 30-46 and col.11, lines 10-12).

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Leynna T. Truvan whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM) and telework on Wednesday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/L. T. T./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435